



Agile Authorization Filters

for

Distributed Information and

Application Access



Enterprises are rapidly providing access to core operational information and applications via web based user interfaces and 'web services' application interfaces. A widening range of stakeholders from employees to external partners need real time, global access in order to support the mission of the organization. Supply chain integration is a powerful example of the expanding scope of access to key information. The information ranges from highly structured information such as schedules, costs, and availability, to unstructured documents. Many applications are making their information available via the web. However, careful consideration needs to be given to managing the access to all of this information.

Historically, various means have been employed to manage access to computing resources and information. The first approach was physical security. The lock on the proverbial 'glass house' door limited access to a few employees. The corporation had to trust them since only they know how to run the computer. Data entry and reports were similarly entrusted to a limited number of trusted employees. In addition to physical security, another tool that actually has played a big part in controlling access and still sees wide use is application complexity. Only the few 'experts' who were given the proper training could understand the information and thus pose a threat. Information was kept in isolated 'silo' applications. Only after the information was assembled and presented to high level management was it combined in a way that could put the company at risk.

As computing moved out to departmental computers, another means of managing authorization was required. People began accessing their computers from their private offices. The increasing numbers of users, users moving in and out of positions requiring access, and the increasing sophistication in the user community greatly increased the need for more advanced security. The most primitive level of automated authentication and authorization that was employed was to allow one or more user accounts to be set up with passwords. Often the ability to set up new accounts was limited to a special 'administrator' account.

When networks were introduced, systems continued to become more integrated and interconnected. Often many users could each have access to multiple applications. Also, the number of changes in who should access each resource continued to increase. The concept of 'role groups' was introduced to address this. The users were assigned to one or more groups. Then, access to applications and other resources can be given to this group. This helped somewhat to manage changes. Other custom approaches such as application specific tokens have also been attempted. However, these usually provide only limited flexibility.



Several approaches were also developed for managing authentication of users who are accessing multiple applications. The goal was to provide a 'single sign on' for the user. Microsoft's Passport and the Liberty alliance are two popular approaches. However, authorization is still usually based on role groups. Some implementations do involve more sophisticated processing related to a user's attributes. However, this still requires the explicit management of authorization information.

Recently, several developments have dramatically increased the need for a more agile approach to managing user authorization. Information and application access and integration within and between Enterprises has begun to increase significantly. Information privacy has become increasingly critical. Users have begun accessing a rapidly increasing range of applications and sensitive information over the internet. Trying to manage user authorization in this environment with traditional approaches is kind of like trying to negotiate the Los Angeles Expressway during rush hour in a golf cart. Telling the user to be more alert is not enough, especially as the changes continue to increase. In this environment, fine-grained authorization management is critical. It must be dynamic and require minimal maintenance.

Agile authorization filters provide an ideal method to manage authorization in this environment. They are designed to interact dynamically with the core information of the enterprise. These filters quickly scan through interrelationships of people, projects, organizational structures, accounts, and historical records to determine exactly what authority a given user should have over a given resource at a given time. As powerful as they are, they are intuitive to define. The person directly responsible for a given resource defines the rules governing its use by others. Then, whenever a given user meets the qualifications for a resource, they have the ability to interact with it as specified.

We will look at an example to illustrate how dynamic filters work. The 'Widget Development Team' has been assembled at ACME Enterprises to develop the new widget, which is a key part of the Gizmo project. Few members of this multi-functional team are dedicated full time. Some are involved in quite a few projects. Several of the team members are working from different international offices. The project's default directory is being used to share general files among the whole team. A management directory will be used by the Widget management team. This will also be accessible by the Gizmo management team so they can be aware of any issues that may affect them. A technical directory will be used by the Widget technical team. Each of these directories will contain files used on the project as well as forums to record notes from online meetings and other discussions. Together, this will provide a virtual project office and eventually a historical record for the project.



Careful controls need to be in place to manage who has authority to manage these 'Widget' resources. Any individual that is assigned to the project needs to have read and write access to the default directory. Only individuals assigned as managers of the project can administer the default directory. Only they can even know about the management directory. Only the technical staff and management have any access to the technical directory. Management of the 'Gizmo' project team also need to have access to the 'Widget' team's resources for an occasional review. Technical staff of the 'Gizmo' project team also needs to have access to the 'Widget' team's technical resources to review technical issues. These basic requirements allow the staff to manage information about their project in an orderly fashion from where ever they are located.

Meeting the above basic requirements using traditional role based security is very cumbersome, even, or especially, if the tool is web based. One approach is to assign each person to each directory, or to each file if directories are not supported. This is obviously very inefficient and leaves tremendous room for inaccuracy. Another approach is to assign people to role groups such as 'General', 'Management', and 'Technical' and then assign these groups to each directory or resource. However, this does not keep people who are 'Management' of one group from accessing 'Management' information in another project where they do not have that role. A second authorization mechanism such as a 'token' could be used for this second level of authorization. However, high-level staff would soon have a very large number of tokens. In addition, every time someone is removed from a project, the token would have to be changed, affecting a large number of people. The alternative is to create a separate role group for each project. Obviously, this also becomes very difficult to manage and requires high maintenance for higher-level individuals who have access to multiple projects.

Some new form of authorization management is needed which provides very fine grained authorization, is very reliable, and yet requires very little maintenance as people and organizational structures change. Agile authorization filters provide this. They move beyond 'role based' authorization to provide 'rule based' authorization. These filters analyze the user and the authorization they are requesting from an agile architectural perspective. This results in fine-grained authorization that ideally supports change and minimizes complexity. Agile authorization filters are applied to document directories, financial processing, performance reports, or any other resource. Each filter can evaluate a user's roles, where they have the role, their training, their certification, etc. along with the current organizational structure to determine what access they should have to the resource.



Agile authorization filters give each person access to the exact information and functionality that is appropriate at a given point of time. For a large organization and especially with value chain integration, each individual can have a unique user experience. Users' experiences will dynamically change as groups change their reporting structure, as projects go through different phases, as individuals gain new training, etc. Most importantly, no system administration effort is required to manage this change. As managers change organizational and project structures, and as individuals receive new training and assignments, the filters dynamically adapt.

The move to distributed information and application management is inevitable for medium to large organizations. A rapidly increasing number of people need to interact with a rapidly increasing range of sensitive information. The authorization requirements for each individual are changing at an every increasing pace. Traditional methods of managing this access simply cannot address the change, complexity, and cost issues. This leads to spiraling cost and tremendous security risks. Agile authorization filters needed to address these challenges. An effective implementation of agile authorization filters can provide access to the exact information and capabilities that are needed when it is needed while reducing management overhead and increasing security.

© Agilize Business Solutions